The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
11/2/2011
11/4/2011 - UPDATED
12/13/2011 - UPDATED

SUBJECT:
Vulnerability in Microsoft Windows Could Allow Remote Code Execution

ORIGINAL OVERVIEW:
A recently identified malicious software, called W32.Duqu or Duqu, has been taking advantage of an unpatched vulnerability in the Microsoft Windows Kernel which is a critical component of a computer operating system that provides basic services for all other parts of the operating system. This vulnerability could allow a remote attacker to take control of a system if a user opens a specially crafted Microsoft Word file. An attacker could then install programs; view, change, or delete data; or create new accounts with full system rights.

November 4 UPDATED OVERVIEW:
Microsoft has released additional information regarding this vulnerability and has provided a work-round.

December 13 UPDATED OVERVIEW:
Microsoft has released a patch for this vulnerability in bulletin MS11-087 (MS-ISAC Advisory 2011-073).

SYSTEMS AFFECTED:

- Microsoft Windows XP
- Microsoft Vista
- Microsoft Windows 7
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

ORIGINAL DESCRIPTION:
A zero-day vulnerability was discovered in the Microsoft Windows Kernel that could result in remote code execution with kernel-level privileges. The researchers responsible for identifying the vulnerability concluded that the Trojan known as W32.Duqu has been successfully exploiting the vulnerability. The University concluded that the Trojan known as W32.Duqu was successfully exploiting the vulnerability. Microsoft has been notified of the vulnerability and is expected to address the issue.

The specifics of this vulnerability are currently unknown at this time. Attackers can exploit this issue by creating a specially crafted Microsoft Word '.doc' file and distributing the file to unsuspecting users. File distribution is likely to occur through attachments or links embedded in email messages. Successful exploitation has been documented to allow remote code execution resulting in the installation of malicious software.

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

November 4 UPDATED DESCRIPTION:
On November 3rd 2011, Microsoft acknowledged a vulnerability in the win32k.syskernel-mode driver. The win32k.sys driver is used by the Microsoft Windows Kernel to manage displays, collect device input, pass information to applications, and display font types. This vulnerability occurs due to the way the win32k.sys driver fails to properly interpret and display TrueType fonts. By default, all affected operating systems support the rendering of TrueType fonts.

An attacker could leverage this vulnerability by creating a specially crafted Microsoft Word '.doc' file and then distributing the file through email or by persuading a user to visit a specially crafted webpage with an embedded TrueType font. Successful exploitation will allow attackers to run arbitrary code with kernel mode privileges. This could allow attackers to install programs; view, change, or delete data; or create new accounts with full user rights.

December 13 UPDATED DESCRIPTION:
Microsoft has released a patch for this vulnerability in bulletin MS11-087 (MS-ISAC Advisory 2011-073).

ORIGINAL RECOMMENDATIONS:
We recommend the following actions be taken:

- When available, apply the appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Apply the principle of Least Privilege to all services.

November 4 UPDATED RECOMMENDATIONS:
The following actions should be taken:

Microsoft has released a workaround that denies access to the vulnerable shared library, T2EMBED.DLL. Instructions on how to apply the workaround can be found here http://support.microsoft.com/kb/2639658

December 13 UPDATED RECOMMENDATIONS:
We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.

ORIGINAL REFERENCES:

Security Focus:
http://www.securityfocus.com/bid/50462/

Symantec:
http://www.symantec.com/connect/w32-duqu_status-updates_installer-zero-day-exploit
http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet

Laboratory of Cryptography and System Security:
http://www.crysys.hu/

November 4 UPDATED REFERENCES:

Microsoft:
http://technet.microsoft.com/en-us/security/advisory/2639658

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3402

December 13 UPDATED REFERENCES:

Microsoft:
http://technet.microsoft.com/en-us/security/bulletin/ms11-087
http://blogs.technet.com/b/srd/archive/2011/12/13/more-information-on-ms11-087.aspx

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3402

SecurityFocus:
http://www.securityfocus.com/bid/50462